4-3

УДК 004.415.24; 004.83; 519.22

В.К. Задирака, Л.Л. Никитенко
Институт кибернетики имени В.М. Глушкова НАНУ, г. Киев, Украина
zvk140@ukr.net

Новые подходы к разработке алгоритмов скрытия информации

В работе рассматривается ряд новых методов встраивания информации в цифровые контейнеры. Условиями, ограничивающими искажение исходного изображения при встраивании информации, являются незаметность искажения для глаза человека и (или) выполнение критерия стойкости стего к пассивным атакам. Подходы к встраиванию информации разделены на три основных направления: использование возможностей цифрового представления изображения, использование элементов и образов самого изображения, использование оптических иллюзий, созданных самими образами или их фонами.

Введение

Работа освещает новые возможные подходы к встраиванию информации в цифровые изображения (ЦИ). В последнее десятилетие началось активное развитие методов встраивания секретных сообщений и водяных знаков в ЦИ [1].

Качество искажения контейнера, вызванного встраиванием, будем оценивать по двум параметрам:
– неотличимость глазом человека пустого контейнера от заполненного;
– выполнение критерия стойкости, основанного на ограничении величины относительной энтропии между распределениями вероятности элементов пустого контейнера и стего.

Как правило, при встраивании используется изменение величин пикселов изображения либо их перестановка. Большинство этих методов оказываются нестеганостойкими, поскольку приводят к увеличению относительной энтропии между пустым контейнером и стего либо не выдерживают визуальных атак.

Разработанные на сегодня алгоритмы скрытия информации в основном используют такие вероятностные характеристики контейнера, как корреляция пикселов и дисперсия величин яркости или цвета пикселов для выбора областей встраивания секретной информации. Само вероятностное распределение яркости пикселов или цвета либо не используется совсем, либо используется в критерии стойкости стего при пассивных атаках или для принятия решения о наличии встроенной информации (например, использование критерия Неймана-Пирсона [2]). Информация, заключенная в самом изображении, не используется для передачи секретного сообщения. Часть информации контейнера может использоваться как цифровой водяной знак, как параметры сообщения или быть самим сообщением. В этом случае искажение контейнера можно значительно уменьшить или устранить полностью.

Величины пикселов, их распределение или другие параметры контейнера могут использоваться для определения параметров нелинейных уравнений, решения которых являются секретным сообщением или его зашифрованной версией. Теория чисел, которая привлекает внимание ученых не одну тысячу лет, может подсказать новые методы использования цифрового представления изображения для создания алгоритмов передачи секретной информации или встраивания водяного знака.

В большом потоке изображений спрятать стеганограмму от противника несложно. При этом возможности человека на глаз определить наличие искажений, которые могут сигнализировать о присутствии встроенной информации, приобретают большое значение. Зрение человека отличается от «зрения», которым может обладать техническое устройство. Человек видит не механически, на его видение существенное влияние оказывают мозг и память. Память человека хранит информацию о перспективе, восстанавливает контуры знакомых фигур, сжимает или растягивает расстояния, в результате чего реальное изображение воспринимается в искаженном виде.

1. Использование возможностей ЦИ

Возможности представления изображения в виде ЦИ уже сегодня используются стеганографией. Подавляющее большинство методов и алгоритмов встраивания используют тот факт, что относительно небольшие изменения величин пикселов изображения остаются незаметными для глаза человека и укладываются в пределы погрешности округления [1], [3], если информация встраивается в коэффициенты какого-либо преобразования изображения. Перестановка пикселов, близких по величине, также используется достаточно широко. Рассмотрим новые идеи использования ЦИ, которые пока не встречались.

1.1. Вероятностный метод

В работах [4], [5] получены условия изменения величин пикселов черно-белого полутонового («серого») изображения, выполнение которых обеспечивает выполнение критерия стойкости. Для цветного изображения эти условия могут накладываться как на изменение величины яркости пикселов, так и на изменения каждой цветовой составляющей.

Для вероятностного метода встраивания секретной информации основой является вероятностное распределение величин пикселов в серых изображениях (распределение уровней яркости или отдельной цветовой составляющей в цветных изображениях). На языке стеганографии его можно называть распределением алфавита в конкретном изображении. Ключом в этом случае является упорядоченная последовательность вероятностей появления пиксела заданной величины. Получатель считывает секретное сообщение непосредственно по изменениям вероятностного распределения алфавита. Встраиванию одного бита информации может соответствовать изменение вероятности появления одной буквы алфавита, вероятности появления слова или вероятности появления букв из некоторого ограниченного множества, принадлежащего алфавиту изображения. Чтобы уменьшить вероятность появления ошибок первого рода (когда ошибочно принимается решение о наличии встроенного бита сообщения), получатель при считывании может использовать пороги обнаружения.

Рассмотрим пример. Пусть алфавит сообщения состоит из 1 и -1. Встраивание одного бита сообщения соответствует изменению вероятности появления одного значения величины пикселов серого изображения (одной буквы алфавита изображения) на величину, превышающую заданный порог T. При встраивании 1 вероятность увеличивается, при встраивании -1 – уменьшается. Множество величин пикселов (алфавит изображения) упорядочено, например, в порядке возрастания, и имеет мощность N.

Приведем пошаговое описание алгоритма.

Первый шаг. **Выбор множества пикселов *M*, величины которых могут меняться незаметно для глаза человека.** Выполняется один раз в начале работы алгоритма. На этом шаге с помощью перцепционной маски, построенной на основе психофизиоло-

гической модели зрения человека, в матрице ЦИ определяются пикселы, которые будут изменяться при встраивании сообщения. Выбираются пикселы высокочастотных участков контейнера, где их распределение наиболее близко к равномерному; выбираются пикселы на границе резкого перепада в их величинах (контуры образов на изображении). Каждый элемент множества M характеризуется координатами в матрице ЦИ (a,b), номером буквы i в алфавите и максимальным возможным изменением величины Δ

$$M = \{m(i,\Delta,a,b)\}.$$

Для встраивания сообщения создается цикл по последовательности букв в упорядоченном алфавите изображения.

Второй шаг. **Расчет дискретного распределения величин пикселов в изображении.** Этот шаг выполняется перед встраиванием каждого бита сообщения. Подсчитывается количество k_i пикселов i-ой величины, и каждой i-ой букве ставится в соответствие вероятность ее появления в матрице ЦИ $F_i = k_i / K$, где K есть общее количество пикселов в матрице ЦИ.

Третий шаг. **Встраивание одного бита сообщения.** Если в i-ю букву алфавита нужно встроить -1, тогда определяется количество пикселов Δ_i, величина которых должна измениться с i-ой буквы на другую букву

$$\Delta_i \geq k_i^{'} - k_i + TK,$$

где k_i и $k_i^{'}$ – количество пикселов i-ой величины в контейнере и в текущем изображении соответственно. Из множества M выбирается Δ_i пикселов, величины которых меняются с i-ой буквы на любую букву, стоящую в алфавите после i-ой буквы.

Если в i-ю букву алфавита нужно встроить 1, тогда определяется количество пикселов Δ_i, величины которых должны измениться с какой-то другой буквы на i-ую букву

$$\Delta_i \geq k_i - k_i^{'} + TK.$$

Из множества M выбирается Δ_i пикселов, величины которых меняются с другой буквы на i-ую.

Изменение величины пиксела не должно превышать значения Δ, определенное для него на первом шаге работы алгоритма.

Если из множества M невозможно выбрать нужное количество пикселов, чтобы встроить данный бит сообщения, то осуществляется переход к следующей букве алфавита.

После встраивания бита сообщения в i-ую букву из множества M исключаются все пикселы, величины которых равны данной букве, и все пикселы, величины которых уже изменились.

Далее осуществляется переход в цикле для встраивания следующего бита сообщения в следующую букву алфавита, пока все сообщение не будет встроено.

Четвертый шаг. **Корректировка.** Выполняется один раз после встраивания сообщения. Пусть сообщение было встроено в N1 букв алфавита. Вероятности оставшихся N-N1 букв в идеале должны совпадать с соответствующими вероятностями контейнера. На практике достаточно добиться того, чтобы изменения этих вероятностей не превышало выбранного порога, тогда при считывании сообщения такие буквы будут просто пропускаться. Если это условие выполняется, то работа алгоритма считается законченной. Иначе осуществляется корректировка вероятностей остатка алфавита. При выполнении корректировки изменяться могут пикселы, которые составляют множество M после встраивания сообщения, в вероятности величин которых встраивание не выполнялось. Вероятности букв изображения, в которые встроена 1, могут увеличиваться. Вероятности букв изображения, в которые встроена -1, могут уменьшаться.

После проведения корректировки работа алгоритма считается оконченной.

Ключом является упорядоченная последовательность F_i, рассчитанная для контейнера.

Вероятностный метод встраивания имеет малую пропускную способность канала, ограниченную размером алфавита изображения и необходимостью использовать информацию обо всех пикселах заданной величины для встраивания одного бита сообщения. Малая пропускная способность метода является платой за увеличение стойкости стего от пассивных атак. Для увеличения пропускной способности изображение может быть разделено на взаимно непересекающиеся части, каждая из которых сама станет контейнером. Такое разделение уменьшит количество пикселов, информация о которых используется для встраивания одного бита сообщения, и одновременно увеличит относительное изменение вероятности появления пиксела заданной величины при изменении величины одного пиксела, т.е. может увеличить относительную энтропию и уменьшить стойкость стего.

Чтобы изменить вероятностное распределение алфавита в изображении, нужно вводить изменения в величины пикселов (или в коэффициенты его вейвлет-преобразования) ЦИ с соблюдением ограничений, наложенных на оба параметра, по которым оценивается искажение изображения. В работе [5] описана одна из возможностей изменения величины пикселов с соблюдением критерия стойкости.

1.2. Встраивание с использованием теории чисел

Методы встраивания могут основываться на представлении чисел в определенной форме, на основах теории делимости, на системах диофантовых уравнений, т.е. уравнений, в которых решения должны быть целыми числами.

Квадрат каждого целого числа может быть представлен суммой квадратов четырех целых чисел. Используя ключ, можно выбрать из цифрового представления изображения некоторую последовательность величин пикселов (или коэффициентов какого-либо преобразования, например, коэффициентов вейвлет-преобразования). В этом случае алфавитом сообщения является алфавит изображения. Алгоритмов передачи последовательности величин пикселов может быть много. Рассмотрим три варианта таких алгоритмов, которые легко могут быть реализованы.

В простейшем случае ключом может быть последовательность координат (номер строки и номер столбца в матрице ЦИ) пикселов, величины которых выбраны для передачи секретного сообщения.

Во втором алгоритме последовательность координат пикселов можно передать с помощью некоторой дискретной функции, осью абсцисс которой являются номера столбцов матрицы ЦИ. На оси ординат находятся номера строк. Пусть последовательность номеров столбцов задана с помощью ключа или номера столбцов перебираются последовательно от первого до последнего. Если для выбранного номера столбца значение функции лежит в ε-окрестности целого числа, которое может быть номером строки матрицы ЦИ, тогда это целое число приравнивается второй координате пиксела, и величина этого пиксела становится следующим элементом искомой последовательности. Если же значение функции оказывается за пределами ε-окрестности целого числа, тогда принимается решение, что в данном столбце нет искомого пиксела. Описание выбранной дискретной функции либо передается ключом, либо ключ указывает на функцию из множества функций, известного и отправителю и получателю.

И в первом, и во втором случае допустимы только пассивные атаки на передаваемое изображение, потому что величины пикселов с нужными координатами не должны искажаться при передаче.

Третьим вариантом передачи последовательности величин пикселов может быть изменение вероятности появления пикселов данной величины, превышающее заданный порог. В таком алгоритме нет связи между величиной и координатой пиксела, поэтому он может оказаться устойчивым даже к некоторым видам активных атак, например, сдвигу или повороту.

Выбранная последовательность величин пикселов преобразуется в число с помощью секретного преобразования, известного отправителю и получателю. Число может использоваться непосредственно как сообщение, может быть шифротекстом с открытым ключом, или может использоваться для разложения в сумму квадратов четырех целых чисел. Такое разложение не однозначно, поэтому наличие дополнительной информации, возможно, секретной, позволит увеличить уровень секретности сообщения. В подобных методах трудно провести четкую грань между криптографией и стеганографией, поскольку секретный ключ может применяться и для извлечения секретной информации, встроенной в стего, и для усиления криптостойкости системы.

Диофант был первым математиком, систематически рассматривавшим неопределенные уравнения, в которых значения неизвестных должны быть обязательно целыми числами [6]. На основе диофантовых уравнений можно разработать алгоритмы передачи секретного сообщения. Наиболее простым представляется определение коэффициентов диофантова уравнения (или системы уравнений) из упорядоченной последовательности величин пикселов, которые выбираются с помощью секретного ключа. Решение диофантова уравнения будет секретным сообщением.

Другой алгоритм может использовать решение диофантовых уравнений первой степени с n неизвестными

$$a_1x_1 + a_2x_2 + ... + a_nx_n = b.$$

Отправитель и получатель могут использовать уравнение из наперед заданного множества диофантовых уравнений. Поскольку число решений такого уравнения либо равно нулю, либо бесконечности, выбор нужного уравнения и его решения тоже должен быть установлен заранее, передан с секретным ключом или считан из принятого изображения. Секретным сообщением может быть вектор поправок к решению диофантова уравнения.

Все предложенные алгоритмы встраивания секретного сообщения основаны на использовании информации, встроенной в контейнер, какого-либо искажения контейнера не происходит (исключение составляет алгоритм, использующий вероятностный метод), пустой контейнер ничем не отличается от стего. Если пустой контейнер не отличим от стего, то распределение параметров контейнера совпадает с распределением параметров стего, и относительная энтропия равна нулю. В соответствии с критерием стойкости из [5] при пассивных атаках такие стегосистемы являются абсолютно стойкими.

2. Использование элементов и образов самого изображения

Методы, использующие элементы и образы самого изображения для встраивания секретного сообщения, основываются на частях изображения, выделенных по некоторому правилу, согласованному заранее получателем и отправителем. Эти методы могут использовать части изображения напрямую, производить некоторую их корректировку или использовать их в качестве дополнения к другой секретной информации.